	Garner Police Department **Written Directive**
	Chapter: 400 - Uniforms/Equipment
	Directive: 430.01 - Computers & Electronic Messaging Devices
Authorized by: Chief Joe Binns	**Effective Date:** June 15, 2021
CALEA Standards: 11.4.4, 41.3.7 (6th Edition)	

430.1.1 - Purpose

The purpose of this directive is to provide employees with guidance on the proper use of Department-owned computers and related electronic messaging systems utilized for purposes of disseminating electronic mail, utilizing services of the Internet, and using related electronic message transmission devices.

430.1.2 - Policy

It is the policy of the Department that all employees abide by the guidelines set forth herein when using computers and services of external databases and information exchange networks, as well as voice mail, mobile data terminals, and related electronic messaging devices.

430.1.3 - Definitions

A. Electronic Messaging Device (EMD): Any computer, electronic mail system, voice mail system, cellular phone, paging system, electronic bulletin board, Internet service, mobile data terminal, or facsimile transmission.

B. System Administrator: The Town employee designated with responsibility for managing all aspects of electronic messaging through individual computers and networks within this Department.

430.1.4 – General Use of EMDs

A. Transmission of electronic messages and information on communications media provided for employees of the Department are to be treated with the same degree of propriety and professionalism as official written correspondence.

B. The Department encourages authorized and trained personnel with access to EMDs to utilize these devices whenever necessary. However, use of any of these devices is a privilege that is subject to revocation based on breaches of this policy.

C. All Department employees are required to sign a document acknowledging their understanding of and their obligation to adhere to the Town of Garner's Technology Policies.

430.1.5 - Prohibitions and Restrictions

A. As it relates to EMDs, employees are prohibited from the following;

1. Viewing, downloading, and/or transmitting materials (other than that required for a police investigation) that involve the use of obscene language, images, jokes, sexually explicit materials,

or messages that disparage any person, group, or classification of individuals is prohibited (whether or not a recipient has consented to or requested such material).

2. Accessing any file or database unless they have a need and a right to such information. Additionally, personal identification and access codes shall not be revealed to any unauthorized source.

3. Downloading or installing any software without prior approval from the System Administrator.

4. Downloading or installing any executable or macro file or other materials from the Internet or other external sources without taking prescribed steps to preclude infection by computer viruses.

5. Violating any copyright and licensing restriction of any software (see 430.1.6).

6. Permitting unauthorized persons to use the Department's electronic mail system.

B. EMDs are designed and intended for conducting business of this agency and are restricted to that purpose with the following exceptions:

1. Infrequent personal use of these devices may be permissible if limited in scope and frequency, if in conformance with other elements of this policy, and if not connected with a profit-making business enterprise or the promotion of any product, service, or cause that is not approved by this agency.

2. Employees may make off-duty personal use of agency computers for professional and career development purposes in keeping with other restrictions of this policy.

C. Employees shall observe copyright restrictions of any documents sent through or stored on electronic mail.

430.1.6 - Importing, Installing Software/Hardware

A. Employees shall not download or install any software or hardware or make modifications or upgrades to any EMD without prior approval from the System Administrator as indicated in 430.1.5. All installation or importing of software or programs shall be conducted under the following guidelines to ensure some protection from computer viruses:

1. Information stored or received on a removable media shall be scanned for viruses prior to installation on any Departmental computer.

2. In no case shall external materials or applications be downloaded directly to any shared (network) drive. When in doubt, employees shall consult the System Administrator for guidance.

3. Employees shall observe the copyright and licensing restrictions of all software applications and shall not copy software from internal or external sources unless legally authorized.

a. Authorized agency employees may remove any software for which proof of licensing (original disks, original manuals, and/or license) cannot be provided.

b. Privately-owned software may be loaded on Department computers if it is necessary for business purposes and is properly licensed. Personal software will be removed if it conflicts with Departmental hardware or software, interferes with the ability of other employees to access or utilize the computer, or occupies excessive storage space needed by the Department.

B. The System Administrator must authorize any hardware enhancements or additions to Department-owned equipment. The System Administrator is responsible for determining proper installation procedures if approved.

430.1.7 - Privacy and Public Record

A. Confidential, proprietary, or sensitive information shall be disseminated only to individuals with a need and right to know and when there is sufficient assurance that appropriate security of such information will be maintained. Such information includes but is not limited to the following:

1. Transmittal of personnel information, such as salary, performance reviews, complaints, grievances, misconduct, disciplinary information, medical records or related information;

2. Criminal history information and confidential informant information; and

3. Intelligence and tactical operations files.

B. Employees are advised that they do not maintain any right to privacy in EMD equipment or its contents. The Department reserves the right to access, for business purposes, any information contained on EMDs and may require employee passwords to files that have been encrypted or password-protected.

C. All communications between or among mobile computers are permitted for official business only. Communications may be monitored and are a matter of public record.

D. All dissemination of confidential, proprietary, or sensitive information shall be done in accordance with Department and Town guidelines ensuring proper encryption and security measures are utilized.

E. It is the responsibility of the employee to follow legal and policy guidelines regarding any communication that constitutes a public record.

430.1.8 - Security and Safety

A. When operating a vehicle, the safe operation of the vehicle is an employee's primary responsibility. Use of the computer is always of secondary importance, and the employee should consider the need to safely stop the vehicle before using the EMD if the use is going to divert the employee's attention from the safe operation of the vehicle.

B. To avoid breaches of security, employees shall log off any personal computer that has access to the Department's computer network, electronic mail system, the Internet, or sensitive information whenever they leave their computer.

C. Employees should keep sensitive information from being viewed by unauthorized persons while it is being displayed on a mobile computer. Closing or obscuring the display is recommended any time an employee is away from the computer.

430.1.9 - Audits

Authorized system administrators will conduct periodic audits of EMDs to assure compliance with Department policy and procedure.